Polynomial systems supported on circuits and dessins d'enfants

Frederic Bihan

POLYNOMIAL SYSTEMS SUPPORTED ON CIRCUITS AND DESSINS D'ENFANTS

FREDERIC BIHAN

Abstract. We study polynomial systems whose equations have as common support a set $\mathcal{C}$ of $n+2$ points in $\mathbb{Z}^n$ called a circuit. We find a bound on the number of real solutions to such systems which depends on n, the dimension of the affine span of the minimal affinely dependent subset of $\mathcal{C}$, and the rank modulo 2 of $\mathcal{C}$. We prove that this bound is sharp by drawing so-called dessins d'enfant on the Riemann sphere. We also obtain that the maximal number of solutions with positive coordinates to systems supported on circuits in $\mathbb{Z}^n$ is $n+1$, which is very small comparatively to the bound given by the Khovanskii fewnomial theorem.

Introduction and statement of the main results

The support of a multivariate polynomial is the set of exponent vectors of the monomials appearing in the polynomial. A polynomial system of n polynomial equations in n variables is supported on $\mathcal{A} \subset \mathbb{Z}^n$ if $\mathcal{A}$ is the common support of each polynomial in the system. A theorem due to Kouchnirenro gives that the number of (simple) solutions in the complex torus $(\mathbb{C}^*)^n$ to a generic polynomial system supported on $\mathcal{A}$ is the volume $v(\mathcal{A})$ of the convex hull of $\mathcal{A}$, normalized so that the unit cube $[0,1]^n$ has volume $n!$.

Here, we consider generic polynomial systems with real coefficients, and are interested in their numbers of real solutions in the real torus $(\mathbb{R}^*)^n$. Contrary to the complex case, the number of real solutions depends on the coefficients of the system, and one of the most important question is to find a sharp upper bound (for related results, see [1, 5, 8, 9] for example). A trivial bound is given by $v(\mathcal{A})$, the number of complex solutions. Another bound due to Khovanskii depends only on the number n of variables and the cardinality of the support $\mathcal{A}$. The above Kuchnirenko result shows immediately that such a bound belongs to the "real world", that is, cannot exist as a bound on the number of complex solutions. The Khovanskii bound is

$$2^n 2^{\binom{|\mathcal{A}|}{2}} \cdot (n+1)^{|\mathcal{A}|},$$

and gives an easy way to construct supports $\mathcal{A}$ for which the Kuchnirenko bound $v(\mathcal{A})$ is not sharp. The Khovanskii bound can be stated alternatively without the term 2^n as a bound on the number of *positive solutions*, which are solutions with positive coordinates.

Since we are interested only in the solutions in the real torus, we have the freedom to translate the support $\mathcal{A}$ by an integral vector and also to choose a basis of the lattice $\mathbb{Z}^n$. A translation by an integral vector corresponds to multiplying each polynomial of the system by a monomial, while a change of basis for the lattice $\mathbb{Z}^n$ corresponds to a monomial change of coordinates (with coefficients 1) for the torus. These operations do not change the number of positive, real and complex solutions. In particular, we will always assume that $0 \in \mathcal{A}$. The *rank modulo 2* of $\mathcal{A}$ is the rank of the reduction modulo 2 of the matrix obtained by putting in columns the non zero elements of $\mathcal{A}$. We will denote it by $rk\,(\bar{\mathcal{A}})$.

If $\mathcal{A} \subset \mathbb{Z}^n$ and $|\mathcal{A}| < n+1$, then $v(\mathcal{A}) = 0$, so that supports with such numbers of elements are not interesting. The first case where $v(\mathcal{A})$ is different from 0 arises when $|\mathcal{A}| = n+1$, and the convex hull of $\mathcal{A}$ is an n-dimensional simplex. This case is easy. The number of positive solutions to such systems is at most 1, so that the number of real solutions is at most 2^n. In fact, the maximal number of real solutions is $2^{n-rk\,(\bar{\mathcal{A}})}$ ([10], see also Lemma 1.3).

The goal of this paper is to obtain similar results in the first non trivial case, when the support is *a circuit*. A circuit is a set $\mathcal{C} \subset \mathbb{Z}^n$ of $n+2$ points which affinely span $\mathbb{R}^n$. It contains an unique minimal affinely dependent subset, and we denote by $m(\mathcal{C})$ the dimension of the affine span of this subset. If $m(\mathcal{C}) = n$, that is, if any proper subset of $\mathcal{C}$ is affinely independent, then $\mathcal{C}$ is called a *non degenerate circuit*. We have $m(\mathcal{C}) = 1$ for example when three points of $\mathcal{C}$ lie on a same line. In [1], the authors consider circuits $\mathcal{C}$ (and also more general supports called near circuits) such that the index of $\mathbb{Z}\mathcal{C}$ in $\mathbb{Z}^n$ is odd. This corresponds to circuits $\mathcal{C} \subset \mathbb{Z}^n$ with $rk\,(\bar{\mathcal{C}}) = n$. They obtain the upper bound $2m(\mathcal{C}) + 1$ on the number of real solutions and also prove that this bound is sharp among systems supported on circuits $\mathcal{C} \subset \mathbb{Z}^n$ with $rk\,(\bar{\mathcal{C}}) = n$. In particular, this gives the sharp bound $2n+1$ which can be attained only with non degenerate circuits. We generalize the results in [1] to arbitrary values of the rank modulo 2. The first result gives sharp bounds on the number of positive solutions. Obviously, multiplying by 2^n such a bound gives a bound on the number of real solutions, which is sharp among systems supported on circuits $\mathcal{C}$ with $rk\,(\bar{\mathcal{C}}) = 0$.

Theorem A. *The number of positive solutions to a generic real polynomial system supported on a circuit $\mathcal{C} \subset \mathbb{Z}^n$ is at most*

$$m(\mathcal{C}) + 1.$$

Therefore, the number of real solutions to a generic real polynomial system supported on a circuit $\mathcal{C} \subset \mathbb{Z}^n$ is at most

$$2^n(m(\mathcal{C}) + 1).$$

Moreover, the first bound, and thus the second bound, is sharp. Namely, for any integer m such that $1 \leq m \leq n$, there exist a circuit $\mathcal{C} \subset \mathbb{Z}^n$ with $m(\mathcal{C}) = m$, and a system supported on $\mathcal{C}$ which has $m+1$ positive solutions.

As a consequence, the number of positive solutions to a generic system supported on a circuit in $\mathbb{Z}^n$ is at most

$$n+1$$

while its number of real solutions is at most

$$2^n \cdot (n+1)$$

and these bounds are sharp and can be attained only with non degenerate circuits.

In particular, as in the case of supports forming a simplex, the Khovansky bound is far from being sharp among systems supported on circuits. Theorem A follows from Proposition 2.1 and Theorem 3.7.

Theorem B. *The number, N, of real solutions to a generic real polynomial system supported on a circuit $\mathcal{C} \subset \mathbb{Z}^n$ satisfies*

(1) *If $rk\,(\bar{\mathcal{C}}) \leq m(\mathcal{C})$, then*
$$N \leq 2^{n-rk\,(\bar{\mathcal{C}})} \cdot \big(m(\mathcal{C}) + rk\,(\bar{\mathcal{C}}) + 1\big)\,.$$

(2) *if $rk\,(\bar{\mathcal{C}}) \geq m(\mathcal{C})$, then*
$$N \leq 2^{n-rk\,(\bar{\mathcal{C}})} \cdot (2m(\mathcal{C}) + 1)\,.$$

Moreover, both these bounds are sharp. Namely, let n, m, R be integers such that $1 \leq m \leq n$ and $0 \leq R \leq n$. If $R \leq m$ (resp. $R \geq m$), there exist a circuit $\mathcal{C} \subset \mathbb{Z}^n$ with $m(\mathcal{C}) = m$, $rk\,(\bar{\mathcal{C}}) = R$, and a system supported on $\mathcal{C}$ whose number of real solutions is the bound in (1) (resp. the bound in (2)).

The bounds in Theorem B look like the bound $2^{n-rk\,(\bar{\mathcal{A}})}$ when $\mathcal{A}$ forms an n-dimensional simplex. However, there is an essential difference in that the sharp bounds in Theorem B do not provide the maximal number of real solutions to systems supported on a *given* circuit. Theorem B follows from Theorem 2.2 and Theorem 3.8.

We consider the eliminant defined in [1] of a system supported on a circuit $\mathcal{C} \subset \mathbb{Z}^n$. Assuming that $\mathcal{C} = \{0, \ell e_1, w_1, \ldots, w_n\} \subset \mathbb{Z}^n$, this eliminant is a univariate polynomial of the form
$$f(x) = x^{\lambda_0} \prod_{i=1}^{t} (g_i(x))^{\lambda_i} - \prod_{i=t+1}^{\nu} (g_i(x))^{\lambda_i},$$
where each polynomial g_i has the form $g_i(x) = a_i + b_i x^{\ell}$ with a_i and b_i non zero real numbers. Here, the coefficients a_i and b_i come from the coefficients of the system while the other numbers are determined by $\mathcal{C}$. The number ν is equal to $m(\mathcal{C})$ if 0 and ℓe_1 belong to the minimal affinely dependent subset of $\mathcal{C}$. If $rk\,(\bar{\mathcal{C}}) \neq 0$, then the integer ℓ can be assumed to be odd. We choose to distinguish the case $rk\,(\bar{\mathcal{C}}) \neq 0$ from the case $rk\,(\bar{\mathcal{C}}) = 0$ for which the number of real solutions is given by the number of positive ones. When $rk\,(\bar{\mathcal{C}}) = n$, it is proved in [1] that the real solutions to the system are in bijection with the real roots of f via the projection onto the first coordinate axis. In general, the real solutions project onto the real roots of f which satisfy sign conditions involving products of polynomials g_i. Moreover, such a real root is the image of $2^{n-rk\,(\bar{\mathcal{C}})}$ solutions to the system, at least when ℓ is odd. The positive solutions project bijectively onto the positive roots of f at which all g_i are positive. We determine the above sign conditions, and prove the upper bounds in Theorem A and B using essentially Rolle's theorem.

Writing the eliminant as $f = P - Q$, we see that the number of real (and positive) solutions is closely related to the arrangement of the roots of P, Q and f, their multiplicities being determined by $\mathcal{C}$. We consider the rational function
$$\phi = f/Q = P/Q - 1 : \mathbb{C}P^1 \to \mathbb{C}P^1.$$

The roots of P, Q and f are the inverse images of -1, ∞ and 0, respectively. These roots lie on the graph

$$\Gamma = \phi^{-1}(\mathbb{R}P^1) \subset \mathbb{C}P^1$$

and we see Γ as an example of so-called *dessin d'enfant*. We use then the observation made in [2, 6] (see also [7]) that polynomials P, Q and $f = P - Q$ with prescribed arrangement and multiplicities of their real roots can be constructed drawing so-called *real rational graphs* on $\mathbb{C}P^1$. The sharpness of the bounds in Theorem A and B is then proved by means of such graphs.

The paper is organized as follows. In Section 1, we define the eliminant f of a system and explain the relation between its real roots and the real (resp. positive) solutions to the system. In Section 2, we prove the upper bounds in Theorem A and B, while in Section 3 we introduce real rational graphs and achieve constructions proving the sharpness of these upper bounds.

Acknowledgements. I'm greatly indebted to Ilia Itenberg and Frank Sottile for their support during these last years. Thanks to Frank Sottile and Erwan Brugallé for useful comments on the first version of this paper. Thanks also to Benoit Bertrand and J. Maurice Rojas for their interest in this work.

1. Elimination

A real polynomial system supported on a circuit

$$\mathcal{C} = \{w_{-1}, w_0, \cdots, w_n\} \subset \mathbb{Z}^n$$

is called *generic* if it has $v(\mathcal{C})$ solutions in $(\mathbb{C}^*)^n$. This forces each solution to be a simple solution. We are interested in the real solutions to such a system, by which we mean solutions in the real torus $(\mathbb{R}^*)^n$.

Translating $\mathcal{C}$ by an integral vector and choosing a basis for the lattice $\mathbb{Z}^n$ if necessary, we may assume without loss of generality that $w_{-1} = 0$, and $w_0 = \ell e_1$ for some positive integer ℓ. Perturbing slightly the system, and using Gaussian elimination, it becomes equivalent to a system of the form

$$S \ : \qquad x^{w_i} = g_i(x_1) \ , \quad i = 1, \ldots, n, \tag{1.1}$$

where $g_i(x_1) = a_i + b_i x_1^\ell$ with a_i, b_i non zero real numbers for $i = 1, \ldots, n$ and $g_1, \ldots, g_n$ have distinct roots. Reordering the vectors $w_1, \ldots, w_n$ if necessary, the affine primitive relation on $\{0, e_1, w_1, \ldots, w_n\}$ can be written as

$$\lambda_0 \, e_1 + \sum_{i=1}^{t} \lambda_i w_i = \sum_{i=t+1}^{\nu} \lambda_i w_i, \tag{1.2}$$

where $1 \leq \nu \leq n$, $\lambda_0, \ldots, \lambda_\nu$ are coprime integers, $\lambda_0 \geq 0$ and $\lambda_1, \ldots, \lambda_\nu > 0$. Note that here we could have $t = 0$ or $t = \nu$ so that one of the two sums collapses to 0. The integer

$$\delta := \lambda_0 + \sum_{i=1}^{t} \lambda_i - \sum_{i=t+1}^{\nu} \lambda_i$$

is (up to sign) the coefficient of $w_{-1} = 0$ in (1.2) (the term δw_{-1} does not appear in (1.2) since it is 0). Multiplying (1.2) by ℓ gives an affine relation on $\mathcal{C}$. Set

$$m(\mathcal{C}) := \nu - \chi(\lambda_0 = 0) - \chi(\delta = 0) \tag{1.3}$$

where $\chi(Y)$ is the boolean truth value of Y: $\chi(Y) = 1$ if Y is true and $\chi(Y) = 0$ otherwise. Then $m(\mathcal{C}) + 2$ is the number of non zero coefficients in the primitive affine relation on $\mathcal{C}$, so that $m(\mathcal{C})$ is the dimension of the affine span of the minimal affinely dependent subset of $\mathcal{C}$. The case $m(\mathcal{C}) = n$ arises when $\mathcal{C}$ is a non degenerate circuit, that is, when any proper subset of $\mathcal{C}$ is affinely independent.

Define the *eliminant* of S to be the following univariate polynomial

$$f(x_1) = x_1^{\lambda_0} \prod_{i=1}^{t} (g_i(x_1))^{\lambda_i} - \prod_{i=t+1}^{\nu} (g_i(x_1))^{\lambda_i}. \tag{1.4}$$

From (1.1) and (1.2), it follows immediately that if $x = (x_1, \ldots, x_n)$ is a solution to S then x_1 is a root of the eliminant f.

Write each vector $w_i = l_i e_1 + v_i$ with $v_i \in \mathbb{Z}^{n-1}$. We get the relations

$$\sum_{i=1}^{t} \lambda_i v_i = \sum_{i=t+1}^{\nu} \lambda_i v_i \tag{1.5}$$

and

$$\lambda_0 + \sum_{i=1}^{t} \lambda_i l_i = \sum_{i=t+1}^{\nu} \lambda_i l_i. \tag{1.6}$$

The fact that $\lambda_0, \ldots, \lambda_\nu$ are coprime and (1.6) gives immediately that $\lambda_1, \ldots, \lambda_\nu$ are also coprime, so that the relation (1.5) is in fact the primitive affine relation on $\{0, v_1, \ldots, v_n\} \subset \mathbb{Z}^{n-1}$. In particular, at least one integer among $\lambda_1, \ldots, \lambda_\nu$ should be odd.

Proposition 1.1 ([1])**.** *Assume that λ_j is odd with $j \in \{1, \ldots, \nu\}$. Then $x = (x_1, \ldots, x_n)$ is a real solution to the system S if and only if x_1 is a real root of f and $(x_2, \ldots, x_n)$ is a real solution to the system*

$$y^{v_i} = g_i(x_1)/x_1^{l_i}\,, \quad i \in \{1, \ldots, n\} \setminus \{j\}.$$

For simplicity, we will often assume that λ_1 is odd and thus apply Proposition 1.1 with $j = 1$. Define

$$B := (v_1, v_2, \ldots, v_n),$$

the $n-1$ by n matrix whose columns are the vectors $v_1, v_2, \ldots, v_n$. Let $\bar{B} \in M_{n-1,n}(\mathbb{Z}/2)$ be the the reduction modulo 2 of B and $rk\,(\bar{B})$ be the rank of $\bar{B}$.

Proposition 1.2. *The number of real solutions to S is equal to $2^{n-1-rk\,(\bar{B})}$ times the number of real roots r of f subjected to the sign conditions*

$$\left(g_1(r)/r^{l_1}\right)^{\epsilon_1} \cdots \left(g_n(r)/r^{l_n}\right)^{\epsilon_n} > 0$$

for any $\epsilon = (\epsilon_1, \ldots, \epsilon_n)$ such that $\bar{\epsilon} \in Ker\,\bar{B}$.

It is worth noting that the number of sign conditions can be reduced to $n - rk\,(\bar{B})$ using a basis of $\mathrm{Ker}\,\bar{B}$.

Before giving the proof, we present the following well-known lemma (see [10]).

Lemma 1.3. *Suppose that $0, u_1, \ldots, u_n \in \mathbb{Z}^n$ form an n-dimensional simplex , and let $\bar{U} \in M_n(\mathbb{Z}/2)$ denote the matrix whose columns contains in this order the reductions modulo 2 of $u_1, \ldots, u_n$. Then the number of real solutions in the torus to the system*

$$x^{u_i} = c_i, \, , \quad i = 1, \ldots, n, \tag{1.7}$$

where c_i is a non zero real number, is

(1) 0 *or* $2^{n-rk(\bar{U})}$ *if the volume of the simplex is even,*
(2) 1 *if this volume is odd.*

Moreover, we have $2^{n-rk(\bar{U})}$ real solutions in the first case if and only if

$$c_1^{\epsilon_1} \cdots c_n^{\epsilon_n} > 0$$

for any $(\epsilon_1, \ldots, \epsilon_n) \in \mathbb{Z}^n$ whose reduction modulo 2 belong to the kernel of $\bar{U}$.

Note that the case 2) is in fact redundant since if the volume of the simplex is odd then the kernel of $\bar{U}$ is reduced to 0, hence $2^{n-rk(\bar{U})} = 1$, and the sign conditions are empty.

Proof. There exist two matrices $L, R \in GL_n(\mathbb{Z})$ and integers $a_1, \ldots, a_n$ such that LUR is the diagonal matrix $D = \mathrm{diag}\,(a_1, \ldots, a_n)$. Let $\tilde{u}_1, \ldots, \tilde{u}_n$ be the columns vectors, in this order, of the matrix LU. The matrix L provides the multiplicative change of coordinates $\tilde{y}_i = \prod_{j=1}^n y_j^{(L^{-1})_{ji}}$, $i = 1, \ldots, n$, of the complex torus. This change of coordinates transforms our system to the system $\tilde{y}^{\tilde{u}_i} = c_i \,, \quad i = 1, \ldots, n$, which has the same number of real (and complex) solutions. Multiplication on the right by R transforms this system to the system

$$\tilde{y}_i^{\,a_i} = d_i \quad \text{with} \quad d_i := \prod_{j=1}^{n} c_j^{R_{ji}} \,, \quad i = 1, \ldots, n. \tag{1.8}$$

This system is equivalent to the previous one since $\tilde{y}_i^{\,a_i} = \prod_{j=1}^n (\tilde{y}^{\tilde{u}_j})^{R_{ji}}$ and $R \in GL_n(\mathbb{Z})$. In particular, the initial system (1.7) and the system (1.8) have the same number of real solutions. This number of real solutions is 0 if $d_i < 0$ for some even a_i, or $2^{n-rk(\bar{D})}$ if $d_i > 0$ for all even a_i. The conclusion is now obvious noting that $rk(\bar{D}) = rk(\bar{U})$ and that the reductions modulo 2 of the vector columns $(R_{1i}, \ldots, R_{n,i})$ for which a_i is even generate the kernel of $\bar{U}$. □

Proof of Proposition 1.2 Assume that λ_1 odd. According to Proposition 1.1, we have to count, for any root r of f, the number of real solutions to

$$y^{v_i} = g_i(r)/r^{l_i} \,, \quad i = 2, \ldots, n. \tag{1.9}$$

Set $c_i(r) := g_i(r)/r^{l_i}$, $i = 1, \ldots, n$. Note that $0, v_2, \ldots, v_n$ form an $(n-1)$-dimensional simplex for otherwise there would be an additional affine relation on $\mathcal{C}$ (so that the convex hull of $\mathcal{C}$ would have dimension $< n$). Let $\bar{U} \in M_{n-1}(\mathbb{Z}/2)$ denote the matrix whose columns contains in this order the reductions modulo 2 of $v_2, \ldots, v_n$. According to Lemma 1.3, the number of solutions to (1.9) is either 0, or $2^{n-1-rk(\bar{U})}$. Moreover, it is $2^{n-1-rk(\bar{U})}$ if and only if

$$c_2(r)^{\epsilon_2}\cdots c_n(r)^{\epsilon_n} > 0$$

for any $(\epsilon_2,\dots,\epsilon_n)$ whose reduction modulo 2 belongs to the kernel of $\bar{U} = (\bar{v_2},\ \dots,\bar{v_n})$.

It follows from the relation (1.5) that the reduction modulo 2 of $\lambda := (\lambda_1,\dots,\lambda_\nu,0,\dots,0)$ belongs to the kernel of $\bar{B}$. Moreover, since λ_1 is odd, the kernel of $\bar{B}$ is the direct sum of $(\mathbb{Z}/2)\cdot\bar{\lambda}$ and the kernel (in $\{0\}\times(\mathbb{Z}/2)^{n-1}$) of $\bar{U}$. This also implies that $rk(\bar{U}) = rk(\bar{B})$. To finish, it remains to see that $f(r) = 0 \Rightarrow c_1(r)^{\lambda_1}\cdots c_\nu(r)^{\lambda_\nu} > 0$. $\square$

Remark 1.4. *As explained at the end of the proof, the sign condition $c_1(r)^{\lambda_1}\cdots c_\nu(r)^{\lambda_\nu} > 0$ given by the affine relation on $\{0,v_1,\dots,v_n\}$ is in fact redundant in Proposition 1.2.*

A *positive* solution is a solution with positive coordinates.

Proposition 1.5. *The number of positive solutions to S is equal to the number of roots r of f subjected to the sign conditions*

$$r > 0\ ,\ g_1(r) > 0\ ,\ \dots\ ,\ g_n(r) > 0.$$

Proof. Assume that λ_1 is odd. According to Proposition 1.1 $(x_1,\dots,x_n)$ is a positive solution to S if and only if x_1 is a positive root r of f and $(x_2,\dots,x_n)$ is a positive solution to

$$y^{v_i} = g_i(r)/r^{l_i}\ ,\quad i = 2,\dots,n. \tag{1.10}$$

As it is well-known, the previous system has a positive solution if and only if $g_i(r)/r^{l_i} > 0$ for $i = 2,\dots,n$, and in this case it has exactly one positive solution. To finish, it remains to note that $f(r) = 0$, $r > 0$ and $g_i(r) > 0$ for $i = 2,\dots,n$ implies that $g_1(r) > 0$. $\square$

2. Upper bounds

Let S be a system as in Section 1 and write the eliminant (1.4) as

$$f = P - Q,$$

where $P(x_1) = x_1^{\lambda_0}\prod_{i=1}^{t}(g_i(x_1))^{\lambda_i}$ and $Q(x_1) = \prod_{i=t+1}^{\nu}(g_i(x_1))^{\lambda_i}$. Consider the rational function

$$\phi := f/Q = P/Q - 1. \tag{2.1}$$

Recall that $m(\mathcal{C})$ is the dimension of the affine span of the minimal affinely dependent subset of $\mathcal{C}$.

Proposition 2.1. *The number of positive solutions to S is no more than $m(\mathcal{C}) + 1$.*

Proof. Let $\mathcal{R}_+$ denote the set of positive roots r of f satisfying $g_1(r) > 0\ ,\ \dots\ ,\ g_n(r) > 0$ and let N denote the number of elements of $\mathcal{R}_+$. The number of positive solutions to S is equal to N by Proposition 1.5. Consider an open interval I formed by two consecutive elements of $\mathcal{R}_+$. This interval contains no root of P and Q (since each g_i has simple real roots). As a consequence, the function ϕ is bounded on I. Moreover, ϕ takes the same value 0 on the endpoints of I. Therefore, by Rolle's theorem, the derivative ϕ' has at least one real root in I. This gives $N-1$ distinct positive roots of ϕ', which are different from the roots of P and Q. The roots of ϕ' are the roots of $P'Q - PQ'$. As noticed in ([1], Proof of Proposition 4.3.), the quotient

$$\frac{P'(x)Q(x) - P(x)Q'(x)}{x^{\lambda_0 - 1}\prod_{i=1}^{\mu}(g_i(x))^{\lambda_i - 1}}, \tag{2.2}$$

or, if $\lambda_0 = 0$, the same quotient but with $\ell - 1$ in place of $\lambda_0 - 1$, is a polynomial H which can be written as $H(x) = h(x^\ell)$ where h is real polynomial of degree $m(\mathcal{C})$ and with non zero constant term. Thus the $N-1$ positive roots of ϕ' different from the roots of P and Q should be roots of H. But H has at most $m(\mathcal{C})$ distinct positive roots, hence $N - 1 \leq m(\mathcal{C})$. $\square$

J. Maurice Rojas informed us that Proposition 2.1 can be obtained from [5] (Lemma 2, Section 3).

Define the matrix A as the matrix obtained by putting (in this order) the vectors $w_0, \ldots, w_n$ in columns

$$A := (w_0, \ldots, w_n) \in M_{n,n+1}(\mathbb{Z}) \tag{2.3}$$

We have by definition $rk\,(\bar{\mathcal{C}}) = rk\,(\bar{A})$, where $\bar{A}$ is the reduction modulo 2 of A. Recall that $w_0 = \ell e_1$ and $w_i = l_i e_1 + v_i$ for $i = 1, \ldots, n$, so that

$$A = \begin{pmatrix} \ell & l_1 & \ldots & l_n \\ 0 & & & \\ \vdots & v_1 & \ldots & v_n \\ 0 & & & \end{pmatrix} \tag{2.4}$$

The lower-right matrix $(v_1, \ldots, v_n)$ is the matrix B that we already defined.

Theorem 2.2. *Let N be the number of real solutions to S.*

(1) *If $rk\,(\bar{\mathcal{C}}) \leq m(\mathcal{C})$, then*

$$N \leq 2^{n - rk\,(\bar{\mathcal{C}})} \cdot \big(m(\mathcal{C}) + rk\,(\bar{\mathcal{C}}) + 1\big).$$

(2) *if $rk\,(\bar{\mathcal{C}}) \geq m(\mathcal{C})$, then*

$$N \leq 2^{n - rk\,(\bar{\mathcal{C}})} \cdot (2m(\mathcal{C}) + 1).$$

Proof. Consider first the case $rk\,(\bar{\mathcal{C}}) = 0$. This corresponds to the case $\mathcal{C} \subset 2\mathbb{Z}^n$. Setting $\tilde{w}_i = w_i/2$, a system supported on $\mathcal{C}$ can be rewritten as a system supported on the circuit $\tilde{\mathcal{C}} = \{0, \tilde{w}_{-1}, \tilde{w}_0, \ldots, \tilde{w}_n\}$ so that the number of real solutions (in the real torus) to the system supported on $\mathcal{C}$ is equal to 2^n times the number of positive solutions to the system supported on $\tilde{\mathcal{C}}$. Obviously, we have $m(\tilde{\mathcal{C}}) = m(\mathcal{C})$. The bound $2^n(m(\mathcal{C}) + 1)$ for the number of real solutions to S follows then from Proposition 2.1.

Suppose now that $rk\,(\bar{\mathcal{C}}) \neq 0$, that is, $\mathcal{C}$ is not contained in $2\mathbb{Z}^n$. Then, it is easy to show the existence of points $w_i, w_j \in \mathcal{C}$ such that $w_i - w_j \notin 2\mathbb{Z}^n$, and w_i belongs to the minimal affinely dependent subset of $\mathcal{C}$. Thus, reordering the points of $\mathcal{C}$ so that w_i becomes w_{-1}

and w_j becomes w_0 if necessary, we can assume that the number ℓ is an odd number, and the coefficient δ is non zero. The fact that ℓ is odd gives that $\bar{A}$ and $\bar{B}$ have isomorphic kernels, so that $rk\,(\bar{\mathcal{C}}) = rk\,(\bar{A}) = rk\,(\bar{B}) + 1$.

Define

$$c(r) := (c_1(r), \ldots, c_n(r)) \quad \text{with} \quad c_i(r) := g_i(r)/r^{l_i}\ , \quad i = 1, \ldots, n.$$

Let $\pi_1, \ldots, \pi_{n-rk\,(\bar{\mathcal{C}})+1}$ be vectors in $\mathbb{Z}^n$ whose reductions modulo 2 form a basis of Ker $\bar{B}$. Then Proposition 1.2 gives that the number of real solutions to S is $2^{n-rk\,(\bar{\mathcal{C}})}$ times the number of real roots r of f subjected to the sign conditions

$$(c(r))^{\pi_i} > 0 \quad \text{for} \quad i = 1, \ldots, n - rk\,(\bar{\mathcal{C}}) + 1. \tag{2.5}$$

Consider the $n - rk\,(\bar{\mathcal{C}})+1$ by n matrix Π whose rows are given by the exponent vectors of the sign conditions (2.5). Taking the Hermite normal form of the reduction modulo 2 of Π, we obtain another basis of Ker $\bar{B}$ producing equivalent sign conditions

$$\begin{array}{rcl} c_{s_1}(r) \cdot \prod_{i>s_1, i\notin\mathcal{S}} (c_i(r))^* & > & 0 \\ c_{s_2}(r) \cdot \prod_{i>s_2, i\notin\mathcal{S}} (c_i(r))^* & > & 0 \\ \vdots & \vdots & \vdots \\ c_{s_{n-rk\,(\bar{\mathcal{C}})+1}}(r) \cdot \prod_{i>s_{n-rk\,(\bar{\mathcal{C}})+1}, i\notin\mathcal{S}} (c_i(r))^* & > & 0 \end{array} \tag{2.6}$$

where $1 \leq s_1 < s_2 < \ldots < s_{n-rk\,(\bar{\mathcal{C}})+1} \leq n$, $\mathcal{S} = \{s_1, \ldots, s_{n-rk\,(\bar{\mathcal{C}})+1}\}$ and the stars are exponents taking values 0 or 1.

It remains to show that the set $\mathcal{R}$ of real roots r of f satisfying the sign conditions (2.6) has at most $m(\mathcal{C})+1+rk\,(\bar{\mathcal{C}})$ elements if $rk\,(\bar{\mathcal{C}}) \leq m(\mathcal{C})$, and at most $2m(\mathcal{C})+1$ elements if $rk\,(\bar{\mathcal{C}}) \geq m(\mathcal{C})$.

First note that the integer ℓ being odd, each g_i has only one real root, that we denote by ρ_i. Moreover, the polynomial H defined in (2.2) has at most $m(\mathcal{C})$ real roots since $H(x_1) = h(x_1^\ell)$ with h polynomial of degree $m(\mathcal{C})$. Let I denote an open (bounded) interval formed by two consecutive elements of $\mathcal{R}$. We claim that I should contain at least one element among $0, \rho_1, \ldots, \rho_\nu$ and the real roots of H. Indeed, if the function $\phi = f/Q$ is bounded on I, then I should contain a real critical point (with finite critical value) of ϕ by Rolle's theorem. The critical points of ϕ with finite critical values are contained in the set formed of 0, the roots $\rho_1, \ldots, \rho_t$ of P and the roots of H (see the proof of Proposition 2.1). If ϕ is not bounded on I, then obviously I should contain a root of Q, that is, a root ρ_i for some $i = t+1, \ldots, \nu$.

There is at most one interval I containing 0 and at most $m(\mathcal{C})$ intervals I containing a real root of H. Let us concentrate now on the intervals I which do no contain 0 but contain a root ρ_i with $i = 1, \ldots, \nu$. The number of such intervals is obviously no more than ν. We claim that this number of intervals is also no more than $rk\,(\bar{\mathcal{C}}) - 1$. Indeed, such an interval I should contain a ρ_i with $i \in \{1,\dots,n\} \setminus \mathcal{S}$, for otherwise some sign condition in (2.6) would be violated at the endpoints of I. The claim follows then as the cardinality of $\{1,\dots,n\} \setminus \mathcal{S}$ is $rk\,(\bar{\mathcal{C}}) - 1$.

Therefore, the number of intervals I formed by two consecutive elements of $\mathcal{R}$ is no more than $1 + m(\mathcal{C}) + rk\,(\bar{\mathcal{C}}) - 1 = m(\mathcal{C}) + rk\,(\bar{\mathcal{C}})$, and no more than $1 + m(\mathcal{C}) + \nu$. Obviously, the number of elements of $\mathcal{R}$ is equal to the number of these intervals I added by one. The bound $m(\mathcal{C}) + rk\,(\bar{\mathcal{C}})$ on the number of intervals I gives thus

$$N \leq 2^{n - rk\,(\bar{\mathcal{C}})} \cdot \big(m(\mathcal{C}) + rk\,(\bar{\mathcal{C}}) + 1\big)\,. \tag{2.7}$$

Consider now the bound $1 + m(\mathcal{C}) + \nu$ on the number of intervals I. We see that if this bound is attained, then the polynomial H has $m(\mathcal{C})$ real roots, and each interval I contains exactly one element among the real roots of H, the roots $\rho_1,\dots,\rho_\nu$, and 0. This forces each of these points to be a critical point of ϕ with even multiplicity (and unbounded critical values for the roots of Q). The $m(\mathcal{C})$ real roots of H are simple roots of H, hence critical points with multiplicity 2 of ϕ. The multiplicity of 0 with respect to ϕ is λ_0, while the multiplicity of ρ_i, $i = 1,\dots,\nu$, with respect to ϕ is $\pm\lambda_i$. Consequently, if the number of intervals I is $1 + m(\mathcal{C}) + \nu$, then $\lambda_0, \lambda_1, \dots, \lambda_\nu$ are even: a contradiction since these numbers are coprime. Hence, the number of intervals I is no more than $m(\mathcal{C}) + \nu$. If λ_0 and δ are both non zero, then $\nu = m(\mathcal{C})$ so that the number of intervals I is no more than $2m(\mathcal{C})$. This gives the bound

$$N \leq 2^{n - rk\,(\bar{\mathcal{C}})} \cdot (2m(\mathcal{C}) + 1)\,. \tag{2.8}$$

Recall that we have assumed at the beginning that $\delta \neq 0$. Hence, it remains to see what happens when $\lambda_0 = 0$. In this case, we have $m(\mathcal{C}) = \nu - 1$ and 0 cannot be a critical point of ϕ. Arguing as before, we obtain then that the number of intervals I is no more than $m(\mathcal{C}) + \nu$. Moreover, if this number is equal to $m(\mathcal{C}) + \nu$, then $\lambda_1,\dots,\lambda_\nu$ are even: a contradiction since $\lambda_1,\dots,\lambda_\nu$ are coprime. Hence, the number of intervals I is no more than $m(\mathcal{C}) + \nu - 1 = 2m(\mathcal{C})$, and we retrieve the bound (2.8). $\square$

3. Real rational graphs and sharpness of bounds

3.1. **Real rational graphs.** This subsection comes from [2] (see also [3, 6, 7]). Consider the function (2.1)

$$\phi = f/Q = P/Q - 1$$

as a rational function $\mathbb{C}P^1 \to \mathbb{C}P^1$. The degree of ϕ coincides with that of f. Define

$$\Gamma := \phi^{-1}(\mathbb{R}P^1).$$

This is a real graph on $\mathbb{C}P^1$ (invariant with respect to the complex conjugation) and which contains $\mathbb{R}P^1$. Each vertex of Γ has even valency, and the multiplicity of a critical point with real critical value of ϕ is half its valency. The graph Γ contains the inverse images of -1, ∞ and 0 which are the sets of roots of P, Q and f, respectively. Denote by the same letter p (resp. q and r) the points of Γ which are mapped to -1 (resp. ∞ and 0). Orient the real axis on the target space via the arrows $-1 \to \infty \to 0 \to -1$ (orientation given by the decreasing order in $\mathbb{R}$) and pull back this orientation by ϕ. The graph Γ becomes an oriented graph, with the orientation given by arrows $p \to q \to r \to p$.

Clearly, the arrangement of the real roots of f, P and Q together with their multiplicities can be extracted from the graph Γ. We encode this arrangement together with the multiplicities by what is called a root scheme.

Definition 3.1 ([2]). *A root scheme is a k-uple $((l_1,m_1),\dots,(l_k,m_k)) \in (\{p,q,r\}\times\mathbb{N})^k$. A root scheme is realizable by polynomials of degree d if there exist real polynomials P and Q such that $f = P - Q$ has degree d and if $\rho_1 < \ldots < \rho_k$ are the real roots of f, P and Q, then $l_i = p$ (resp. q, r) if ρ_i is root of P (resp. Q, f) and m_i is the multiplicity of ρ_i.*

Conversely, suppose we are given a real graph $\Gamma \subset \mathbb{C}P^1$ together with a real continuous map $\varphi : \Gamma \to \mathbb{R}P^1$. Denote the inverse images of -1, ∞ and 0 by letters p, q and r, respectively, and orient Γ with the pull back by φ of the above orientation of $\mathbb{R}P^1$. This graph is called *a real rational graph* [2] if

- any vertex of Γ has even valence,
- any connected component of $\mathbb{C}P^1 \setminus \Gamma$ is homeomorphic to an open disk,

Then, for any connected component D of $\mathbb{C}P^1 \setminus \Gamma$, the map $\varphi_{|\partial D}$ is a covering of $\mathbb{R}P^1$ whose degree d_D is the number of letters p (resp. q, r) in ∂D. We define the *degree* of Γ to be half the sum of the degrees d_D over all connected components of $\mathbb{C}P^1 \setminus \Gamma$. Since φ is a real map, the degree of Γ is also the sum of the degrees d_D over all connected components D of $\mathbb{C}P^1 \setminus \Gamma$ contained in one connected component of $\mathbb{C}P^1 \setminus \mathbb{R}P^1$.

Proposition 3.2 ([2, 6]). *A root scheme is realizable by polynomials of degree d if and only if it can be extracted from a real rational graph of degree d on $\mathbb{C}P^1$.*

Let us explain how to prove the if part in Proposition 3.2 (see [2, 3, 6, 7]). For each connected component D of $\mathbb{C}P^1 \setminus \Gamma$, extend $\varphi_{|\partial D}$ to a, branched if $d_D > 1$, covering of one connected component of $\mathbb{C}P^1 \setminus \mathbb{R}P^1$, so that two adjacent connected components of $\mathbb{C}P^1 \setminus \Gamma$ project to differents connected components of $\mathbb{C}P^1 \setminus \mathbb{R}P^1$. Then, it is possible to glue continuously these maps in order to obtain a real branched covering $\varphi : \mathbb{C}P^1 \to \mathbb{C}P^1$ of degree d. The map φ becomes a real rational map of degree d for the standard complex structure on the target space and its pull-back by φ on the source space. There exist then real polynomials P and Q such that $f = P - Q$ has degree d and $\varphi = f/Q = P/Q - 1$, so that the points p (resp. q, r) correspond to the roots of P (resp. Q, f) and $\Gamma = \varphi^{-1}(\mathbb{R}P^1)$.

As in [2], we will abbreviate a sequence S repeated u times in a root scheme by S^u. If $u = 0$, then S^u is the empty sequence.

3.2. **Constructions.** We are going to prove the existence of root schemes by constructing real rational graphs Γ on $\mathbb{C}P^1$. Since these graphs are real, only half of them will be drawn and the horizontal line will represent the real axis $\mathbb{R}P^1$.

Proposition 3.3. *For any even integer $n = 2k > 0$, the root scheme*

$$\big([(q,2),(p,2)]^k,(q,1),(r,1)^{2k+1},(p,1)\big)$$

is realizable by polynomials of degree $n+1$.

For any odd integer $n = 2k+1 > 0$, the root scheme

$$\big([(q,2),(p,2)]^k,(q,2),(p,1)(r,1)^{2k+2},(p,1)\big)$$

is realizable by polynomials of degree $n+1$.

Proof. According to Proposition 3.2, it suffices to construct a real rational graph Γ_{n+1} of degree $n+1$ on $\mathbb{C}P^1$ from which the desired root scheme can be extracted. This is done in Figure 1 for $n = 2, 4$ and in Figure 2 for $n = 3, 5$. These figures provide the induction step $n \to n+2$ for constructing suitable graphs Γ_{n+1} for any positive integer n. □

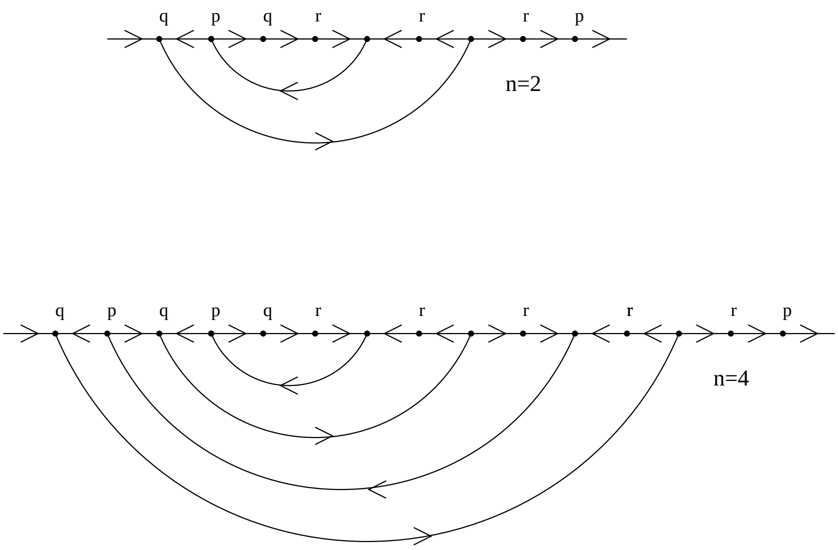

FIGURE 1.

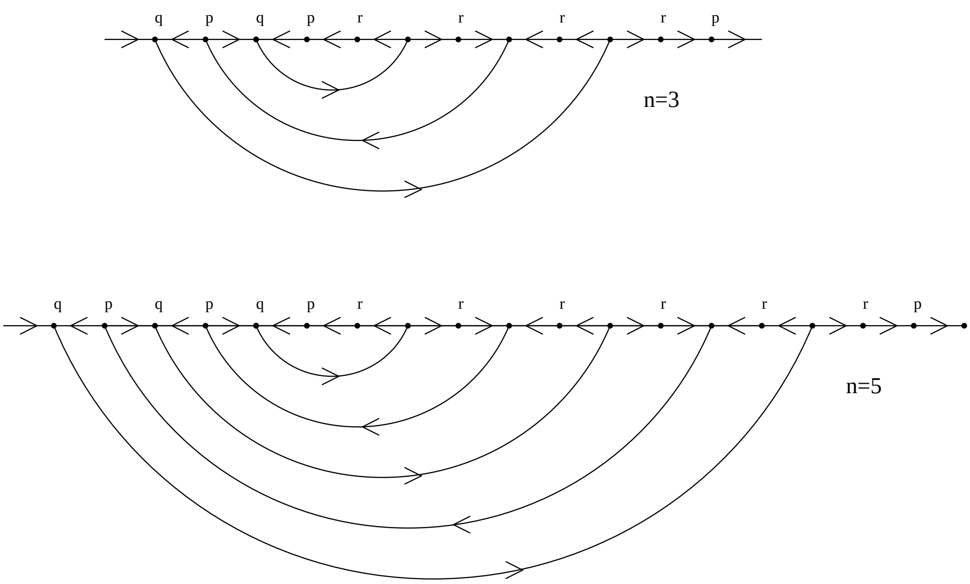

FIGURE 2.

Let n and R be integers such that $0 < R \leq n$. If $n - R$ is even, define I and J by

$$I := [(p,2),(q,2)]^{\frac{n-R}{2}},(q,3),(r,1),(p,2),(r,1)^{n-R+1}$$

$$J := \begin{cases} (r,1),(p,1) & \text{if } R=1 \\ (r,1)^R,(q,2),[(r,1),(p,4),(r,1),(q,4)]^{\frac{R}{2}-1},(r,1),(p,3) & \text{if } R \text{ is even} \\ (r,1)^R,(p,2),[(r,1),(q,4),(r,1),(p,4)]^{\frac{R-3}{2}},(q,4),(r,1),(p,3) & \text{if } R \text{ is odd} \end{cases}$$

If $n - R$ is odd, define

$$I := [(p,2),(q,2)]^{\frac{n-R-1}{2}},(p,2),(q,3),(r,1),(p,2),(r,1)^{n-R+1}$$

$$J := \begin{cases} (r,1),(q,1) & \text{if } R=1 \\ (r,1)^R,(p,2),[(r,1),(q,4),(r,1),(p,4)]^{\frac{R}{2}-1},(r,1),(q,3) & \text{if } R \text{ is even} \\ (r,1)^R,(q,2),[(r,1),(p,4),(r,1),(q,4)]^{\frac{R-3}{2}},(p,4),(r,1),(q,3) & \text{if } R \text{ is odd} \end{cases}$$

Note that the definitions of J with $n - R$ odd and with $n - R$ even are obtained from each other by permuting p and q.

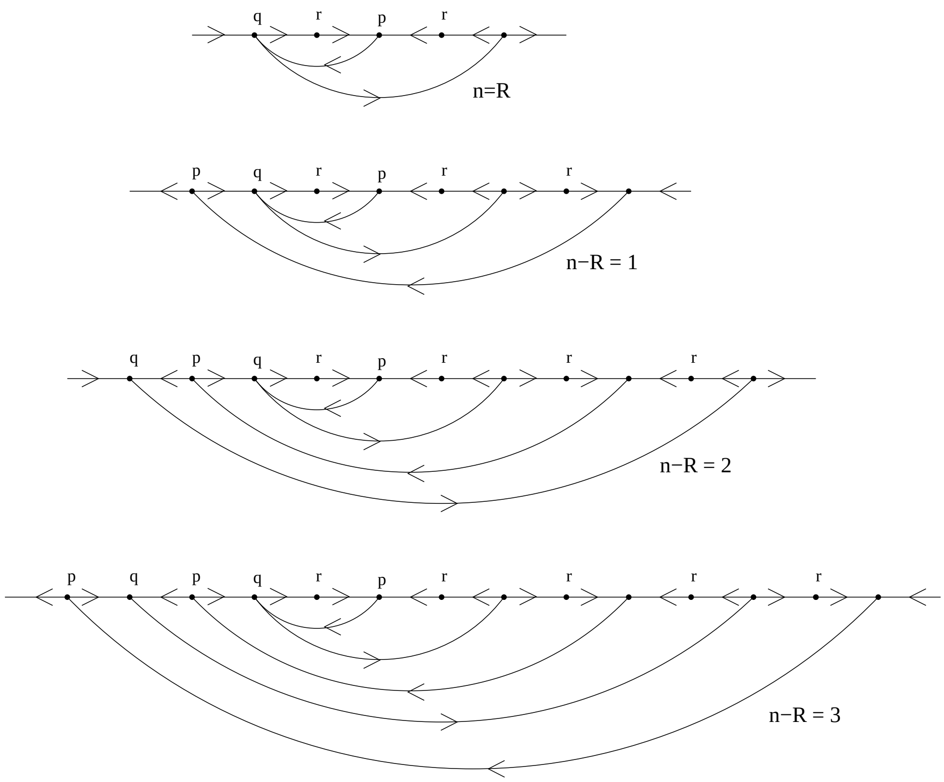

FIGURE 3: GRAPH Γ_I.

Proposition 3.4. *For any integers n and R such that $0 < R \leq n$, the root scheme $(I\ ,\ J)$ is realizable by polynomials of degree $n + R + 1$.*

Proof. First, we contruct graphs Γ_I and Γ_j, which are not real rational graphs, but from which the sequences I and J can be extracted, respectively. Figure 3 shows Γ_I for $n - R = 0, 1, 2, 3$, and indicates how to construct Γ_I for any integer value of $n - R$ with $0 \leq n - R < n$. Similarly, Figure 4 shows Γ_J for $R = 1, 2, 3, 4$ and $n - R$ even, and indicates how to construct Γ_J for any integers n and R such that $0 < R \leq n$ and $n - R$ is even. The graph Γ_J for $n - R$ odd is obtained from the graph Γ_J with $n - R$ even and the same value of R by permuting p and q and reversing all the arrows. For any integers n and R such that $0 < R \leq n$ we can glue the corresponding Γ_I and Γ_J in order to obtain a real rational graph of degree $n + R + 1$ whose root scheme is $(I\ ,\ J)$ (see Figure 5 for $n = 4$ and $R = 3$). The result follows then from Proposition 3.2. $\square$

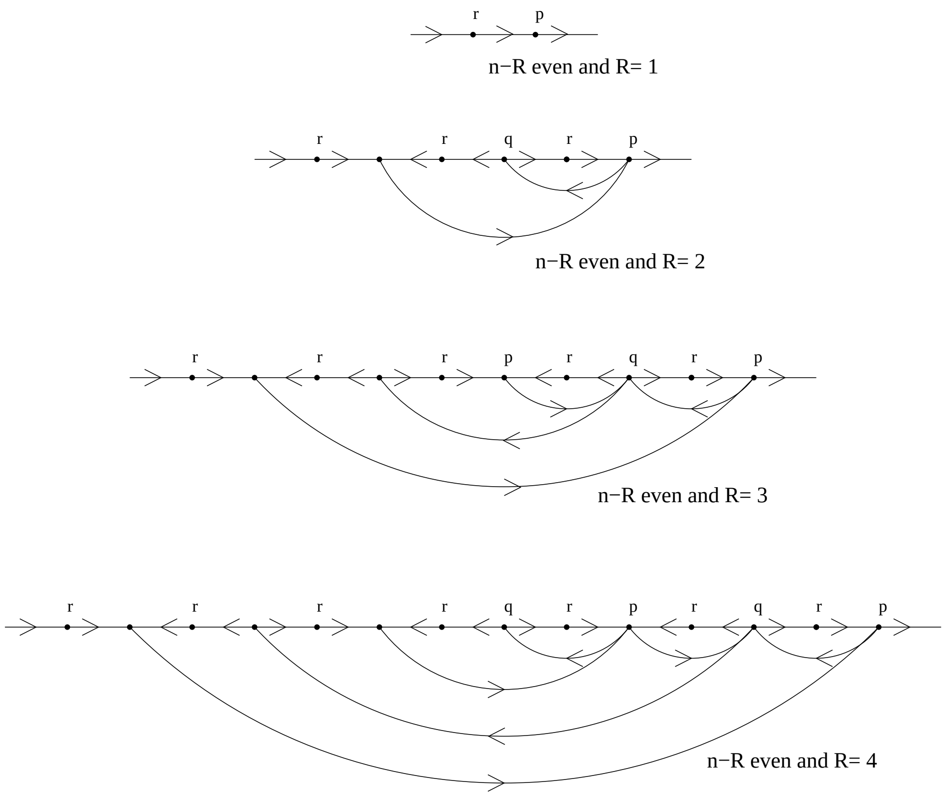

FIGURE 4: GRAPH Γ_J.

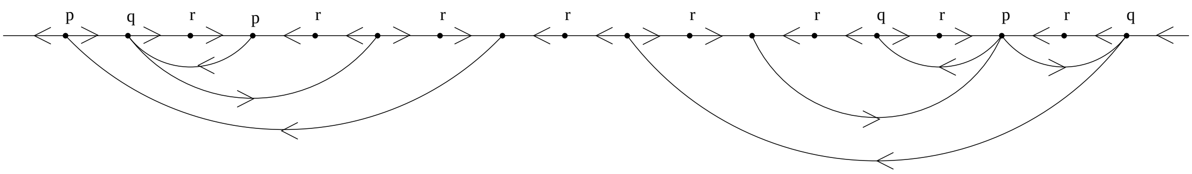

FIGURE 5: GLUING OF Γ_I AND Γ_J FOR $n = 4,\ R = 3$.

3.3. Sharpness of bounds.

Proposition 3.5. *For any positive integer n, there exist a non degenerate circuit $\mathcal{C} \subset \mathbb{Z}^n$ and a generic real polynomial system supported on $\mathcal{C}$ whose number of positive solutions is equal to $n+1$.*

Proof. We prove only the case n even since the case n odd is similar (the case $n=1$ is trivial). So assume that $n = 2k > 0$ is even. According to Proposition 3.3, there exist polynomials P and Q such that $f = P - Q$ has degree $n+1$ and the corresponding root scheme is

$$\left([(q,2),(p,2)]^k,(q,1),(r,1)^{2k+1},(p,1)\right).$$

Composing on the right $\phi = f/Q = P/Q - 1$ with a real automorphism of $\mathbb{C}P^1$ (a real rational map of degree 1), we can choose three values for the points is in this root scheme. Reading the above scheme from the left to the right, we choose $p=0$ for the last but one p, a positive value for the last q, and $p=\infty$ for the last p. This gives the following arrangement of the roots of P, Q and f (where we naturally omit the root at infinity)

$$q_1 < p_1 < \ldots < q_k < p_k = 0 < q_{k+1} < r_1 < r_2 < \ldots < r_{2k+1},$$

so that $f = P - Q$ with

$$P(x) = ax^2(x-p_1)^2 \cdots (x-p_{k-1})^2 \ , \quad Q(x) = b(x-q_{k+1})(x-q_1)^2 \cdots (x-q_k)^2,$$

and $f = P - Q$ has $n+1 = 2k+1$ positive roots which are bigger than the roots of P and Q. Note that $ab > 0$ for otherwise the polynomial $f = P - Q$ could not have roots bigger than the roots of P and Q. Dividing f by a and setting $g_1(x) = x - p_1, \ldots, g_{k-1} = x - p_{k-1}$, $g_k(x) = x - q_1, \ldots, g_{n-1}(x) = x - q_k$ and $g_n(x) = b(x - q_{k+1})/a$, we obtain a polynomial f of the form (1.4) with $\ell = 1$, the exponents are coprime, and such that $\mathcal{R}_+$ has $n+1$ elements. Let us now give explicitely a non degenerate circuit $\mathcal{C} \subset \mathbb{Z}^n$ and then a system (1.1) whose eliminant is f. Take the circuit $\mathcal{C}$ with $w_{-1} = 0$, $w_0 = e_1$, $w_1 = e_2, \ldots, w_{n-1} = e_n$ and $w_n = 2(e_1 + e_2 + \ldots + e_k - e_{k+1} - \ldots - e_n)$. The primitive affine relation on $\{e_1, w_1, \ldots, w_n\}$ is

$$2e_1 + 2(w_1 + \ldots + w_{k-1}) = 2(w_k + \ldots + w_{n-1}) + w_n$$

and has the desired coefficients. Hence $f(x_1)$ is the eliminant of the system $x^{w_i} = g_i(x_1)$, $i = 1, \ldots, n$, given explicitely by

$$\begin{cases} x_2 = x_1 - p_1 \quad , \ \ldots \ , \ x_k = x_1 - p_{k-1} \\ x_{k+1} = x_1 - q_1 \ , \ \ldots \ , \ x_n = x_1 - q_k \\ \left(\frac{x_1 \cdots x_k}{x_{k+1} \cdots x_n}\right)^2 = b(x_1 - q_{k+1})/a. \end{cases}$$

According to Proposition 1.5, this system has $n+1$ positive solutions. □

It may be interesting to note that the previous system has in fact only these $n+1$ positive solutions as solutions in the complex torus. To see this, one can compute that the volume of the circuit is $n+1$, and use Kouchnirenko theorem.

Proposition 3.6. *For any integers n and R such that $0 \leq R \leq n$, there exist a non degenerate circuit $\mathcal{C} \subset \mathbb{Z}^n$ with $rk\,(\bar{\mathcal{C}}) = R$, and a generic real polynomial system supported on $\mathcal{C}$ whose number of real solutions is equal to $2^{n-R}(n+R+1)$.*

Proof. Note that for $R = 0$ this follows from Proposition 1.5 (see the proof of Theorem 2.2). We will give the proof only when n and R are even since the other cases are similar (the case $n = 1$ is trivial).

So let n and R be even integers such that $0 < R \leq n$. According to Proposition 3.4, there exist polynomials P and Q such that $f = P - Q$ has degree $n + R + 1$ and the corresponding root scheme is

$$\Big([(p,2),(q,2)]^{\frac{n-R}{2}},(q,3),(r,1),(p,2),(r,1)^{n+1},(q,2),[(r,1),(p,4),(r,1),(q,4)]^{\frac{R}{2}-1},(r,1),(p,3)\Big).$$

We may choose three values for the roots in this root scheme. Choose $p = 0$ for the p in the sequence $(q,3),(r,1),(p,2)$, a negative value for the r in the same sequence, and the infinity value for the last p on the right in the root scheme. Then, the polynomials P and Q can be written as

$$P(x) = x^2 \prod_{i=1}^{\frac{n-R}{2}} (g_i(x))^2 \cdot \prod_{i=\frac{n-R}{2}+1}^{\frac{n}{2}-1} ((g_i(x))^4,$$

$$Q(x) = (g_{\frac{n}{2}}(x))^3 \cdot \prod_{i=\frac{n}{2}+1}^{n-\frac{R}{2}+1} (g_i(x))^2 \cdot \prod_{i=n-\frac{R}{2}+2}^{n} ((g_i(x))^4$$

so that

($\star$) *$f = P - Q$ has $n + R + 1$ (non zero) real roots, all but one are positive, and g_i is positive at the real roots of f for $i = 1, \ldots, \frac{n-R}{2}$ and $i = \frac{n}{2}, \ldots, n - \frac{R}{2}$.*

Here the g_i have all, but one, the form, $g_i(x) = x - \rho_i$ with ρ_i a finite non zero root p if $i < \frac{n}{2}$ and a root q otherwise. The last one is of the form $c(x - \rho_i)$ where c is a positive real number due to the fact f has a real root bigger than the roots of P and Q (see the proof of Proposition 3.5). The polynomials g_i mentioned in ($\star$) correspond to the sequence $[(p,2),(q,2)]^{\frac{n-R}{2}},(q,3)$ on the left of the above root scheme.

Now, define $v_{n-\frac{R}{2}+1} = -(e_2 + \ldots + e_{n-1}) - 3e_n$, $v_{\frac{n}{2}} = 2(e_2 + \ldots + e_n)$, and

$$\begin{aligned} v_i &= 2e_{i+1}\ , \quad i = 1, \ldots, \tfrac{n-R}{2} \\ v_i &= e_{i+1}\ , \quad i = \tfrac{n-R}{2} + 1, \ldots, \tfrac{n}{2} - 1 \\ v_i &= -2e_i\ , \quad i = \tfrac{n}{2} + 1, \ldots, n - \tfrac{R}{2} \\ v_i &= -e_{i-1}\ , \quad i = n - \tfrac{R}{2} + 2, \ldots, n \end{aligned}$$

The primitive affine relation on $\{0, v_1, \ldots, v_n\}$ is the desired one

$$2\sum_{i=1}^{\frac{n-R}{2}} v_i + 4\sum_{i=\frac{n-R}{2}+1}^{\frac{n}{2}-1} v_i = 3v_{\frac{n}{2}} + 2\sum_{i=\frac{n}{2}+1}^{n-\frac{R}{2}+1} v_i + 4\sum_{i=n-\frac{R}{2}+2}^{n} v_i,$$

and it's easy to see that the rank of the matrix $\bar{B} = (\bar{v}_1, \ldots, \bar{v}_n)$ is $R-1$. We want to find integers $l_1, \ldots, l_n$ verifying the relation (1.6) and such that the sign conditions in Proposition 1.2 are verified at each root r of f. Here, these sign conditions are given by the v_i which belong to $2\mathbb{Z}^n$

$$g_i(r)/r^{l_i} > 0 \quad , \quad i = 1, \ldots, \tfrac{n-R}{2} \quad \text{and} \quad i = \tfrac{n}{2}, \ldots, n - \tfrac{R}{2} \tag{3.1}$$

In view of property $(\star)$, we want to have l_i even for $i = 1, \ldots, \frac{n-R}{2}$ and $i = \frac{n}{2}, \ldots, n - \frac{R}{2}$ since one root of f is negative. In fact we can find integers l_i which are all even. Indeed, in our situation, the relation (1.6) is

$$2 + 2\sum_{i=1}^{\frac{n-R}{2}} l_i + 4 \sum_{i=\frac{n-R}{2}+1}^{\frac{n}{2}-1} l_i = 3l_{\frac{n}{2}} + 2 \sum_{i=\frac{n}{2}+1}^{n-\frac{R}{2}+1} l_i + 4 \sum_{i=n-\frac{R}{2}+2}^{n} l_i. \tag{3.2}$$

Replacing the first 2 on the left by 1, the existence of integers l_i verifying the resulting relation is due to the fact that $2, 4, 3$ are coprime. Multiplying then by 2 the members of this modified relation gives then the existence of even integers l_i verifying (3.2).

So, let us choose even integers l_i verifying (3.2) so that the sign conditions (3.1) are satisfied. The proof is almost finished.

Consider the system

$$x^{w_i} = g_i(x_1) \ , \quad i = 1, \ldots, n, \tag{3.3}$$

where $w_i := l_i e_1 + v_i$. This system is equivalent to a (generic) system supported on the circuit $\mathcal{C} = \{w_{-1} = 0, w_0 = e_1, w_1, \ldots, w_n\}$. The primitive affine relation on $\mathcal{C}$ is

$$2w_0 + 2\sum_{i=1}^{\frac{n-R}{2}} w_i + 4 \sum_{i=\frac{n-R}{2}+1}^{\frac{n}{2}-1} w_i = 3w_{\frac{n}{2}} + 2 \sum_{i=\frac{n}{2}+1}^{n-\frac{R}{2}+1} w_i + 4 \sum_{i=n-\frac{R}{2}+2}^{n} w_i,$$

so that f is the eliminant of (3.3). The rank modulo 2 of $\mathcal{C}$ is $rk\,(\bar{\mathcal{C}}) = rk\,(\bar{B})+1 = R$. The eliminant f has $n+R+1$ real roots and the sign conditions (3.1) are satisfied at each real root of f. Therefore, according to Proposition 1.2 , the system (3.3) has $2^{n-R}(n+R+1)$ real solutions. □

The case $R = n$ in Proposition 3.6 has already been obtained in [1] by different methods.

Theorem 3.7. *For any integers n, m such that $1 \leq m \leq n$, there exist a circuit $\mathcal{C} \subset \mathbb{Z}^n$ with $m(\mathcal{C}) = m$ and a generic real polynomial system supported on $\mathcal{C}$ whose number of positive solutions is $m+1$*

Proof. By Proposition 3.5, there exists a circuit $\mathcal{C}' = \{0, w_0 = \ell e_1, w_1, \ldots, w_m\} \subset \mathbb{Z}^m$ with $m(\mathcal{C}') = m$ and polynomials $g_1, \ldots, g_m$ such that the system $x^{w_i} = g_i(x_1)$, $i = 1, \ldots, m$, has $m+1$ positive solutions. By Proposition 1.5, this means that the eliminant f of this system has $m+1$ positive roots at which $g_1, \ldots, g_m$ are positive. Define

$$w_i := e_i \ , \quad i = m+1, \ldots, n,$$

and choose polynomials $g_{m+1},\dots,g_n$ (as in (1.1)) which are positive at the real roots of f. Then, the system $x^{w_i}=g_i(x_1)$, $i=1,\dots,n$, is equivalent to a system supported on the circuit $\mathcal{C}=\{0,w_0=\ell e_1,w_1,\dots,w_n\}\subset\mathbb{Z}^n$. The eliminant of this system is also f and we have $m(\mathcal{C})=m(\mathcal{C}')=m$. Proposition 1.5 and our choice of $g_{m+1},\dots,g_n$ implies that this system has also $m+1$ positive solutions. □

Theorem 3.8. *For any integers n,m,R such that $0\leq R\leq n$ and $1\leq m\leq n$, there exist a circuit $\mathcal{C}\subset\mathbb{Z}^n$ with $m(\mathcal{C})=m$, $rk\,(\bar{\mathcal{C}})=R$, and a generic real polynomial system supported on $\mathcal{C}$ whose number of real solutions, N, verifies:*

(1) *if $R\leq m$, then*
$$N=2^{n-R}\cdot(m+R+1)\,.$$
(2) *if $R\geq m$, then*
$$N=2^{n-R}\cdot(2m+1)\,.$$

Proof. The case $R=0$ is an immediate consequence of Theorem 3.7. Suppose that $0<R\leq m$. By Proposition 3.6, there exist a circuit $\mathcal{C}'=\{0,w_0=\ell e_1,w_1,\dots,w_m\}\subset\mathbb{Z}^m$ with $m(\mathcal{C}')=m$, $rk\,(\bar{\mathcal{C}}')=R$, and polynomials $g_1,\dots,g_m$ such that the system

$$x^{w_i}=g_i(x_1)\ ,\quad i=1,\dots,m, \tag{3.4}$$

has $2^{m-R}\cdot(m+R+1)$ real solutions. Here and in the rest of the proof g_i is a polynomial as in (1.1). Since $rk\,(\bar{\mathcal{C}}')\neq 0$, we may assume that ℓ is odd. Define

$$w_i:=2e_i\ ,\quad i=m+1,\dots,n,$$

and choose polynomials $g_{m+1},\dots,g_n$ which are positive at the real roots of the eliminant f of (3.4). Then, the system

$$x^{w_i}=g_i(x_1)\ ,\quad i=1,\dots,n, \tag{3.5}$$

is equivalent to a system supported on the circuit $\mathcal{C}=\{0,w_0=\ell e_1,w_1,\dots,w_n\}\subset\mathbb{Z}^n$. We have $m(\mathcal{C})=m(\mathcal{C}')=m$, $rk\,(\bar{\mathcal{C}})=rk\,(\bar{\mathcal{C}}')=R$ and f is also the eliminant of (3.5). Moreover the sign conditions in Proposition 1.2 which correspond to (3.5) are obtained from those corresponding to (3.4) by adding $g_i(r)>0$ for $i=m+1,\dots,n$ (note that $l_{m+1}=\dots=l_n=0$). But since (3.4) has $2^{m-R}\cdot(m+R+1)$ real solutions, and ℓ is odd, it follows from Proposition 1.2 that the sign conditions corresponding to (3.4) are satisfied at $m+R+1$ real roots of f. By our choice of $g_{m+1},\dots,g_n$, the sign conditions corresponding to (3.5) are satisfied at the same $m+R+1$ real roots of f. Hence, again by Proposition 1.2, the system (3.5) has $2^{n-R}\cdot(m+R+1)$ real solutions.

Finally, suppose that $R>m$. The idea is exactly as before. By Proposition 3.6, there exist a circuit $\mathcal{C}'=\{0,w_0=\ell e_1,w_1,\dots,w_m\}\subset\mathbb{Z}^m$ with $m(\mathcal{C}')=m$, $rk\,(\bar{\mathcal{C}}')=m$ and polynomials $g_1,\dots,g_m$ such that the system (3.4) has $2m+1$ real solutions. According to Proposition 1.2 (see also Remark 1.4), this means that the eliminant f of this system has $2m+1$ real roots. Define

$$w_i:=e_i\ ,\quad i=m+1,\dots,R,\quad w_i:=2e_i\ ,\quad i=R+1,\dots,n$$

and choose polynomials $g_{R+1},\dots,g_n$ which are positive at the roots of the eliminant f. Then, the system (3.5) is equivalent to a system supported on the circuit $\mathcal{C}=\{0,w_0=$

$\ell e_1, w_1, \ldots, w_n\} \subset \mathbb{Z}^n$. We have $m(\mathcal{C}) = m$, $rk\,(\bar{\mathcal{C}}) = R$ and (3.5) has $2^{n-R} \cdot (2m+1)$ real solutions. $\square$

References

[1] B. Bertrand, F. Bihan, and F. Sottile, *Polynomial Systems with Few Real Zeroes*, ArXiv:math.AG/0502051, to appear in Math. Zeitschrift.

[2] E. Brugallé, *Real plane algebraic curves with asymptotically maximal number of even ovals*, ArXiv:math.AG/0411097, to appear in Duke Mathematical Journal.

[3] E. Brugallé, *Courbes algébriques réelles et courbes pseudoholomorphes réelles dans les surfaces réglées*, Phd thesis, University of Rennes 1, France, (2004), (in english), http://tel.ccsd.cnrs.fr/documents/archives0/00/00/86/52/.

[4] A.G. Kouchnirenko, *A Newton polyhedron and the number of solutions of a system of k equations in k unknowns*, Usp. Math. Nauk. **30** (1975), 266–267.

[5] Tien-Yien Li, J. Maurice Rojas, and Xiaoshen Wang,*Counting real connected components of trinomial curve intersections and m-nomial hypersurfaces*, Discrete Comput. Geom. **30** (2003), no. 3, 379–414. MR 2 002 964

[6] S. Yu Orevkov, *Riemann existence theorem and construction of real algebraic curves*, Ann. Fac. Sci. Toulouse Math. (6) **12** (2003), no. 4, 517–531.

[7] S. Natanzon, B. Shapiro, and A. Vainshtein, *Topological classification of generic real rational functions*, J. Knot Theory Ramifications **11** (2002), no. 7, 1063–1075.

[8] F. Sottile, *Enumerative real algebraic geometry*, Algorithmic and quantitative real algebraic geometry (Piscataway, NJ, 2001), 139–179, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 60, Amer. Math. Soc., Providence, RI, 2003.

[9] E. Soprunova, F. Sottile, *Lower bounds for real solutions to sparse polynomial systems*, ArXiv:math.AG/0409504, to appear in Advances in Mathematics.

[10] B. Sturmfels, *On the number of real roots of a sparse polynomial system*, Hamiltonian and gradient flows, algorithms and control, 137–143, Fields Inst. Commun., 3, Amer. Math. Soc., Providence, RI, 1994.

Laboratoire de Mathématiques, Université de Savoie, 73376 Le Bourget-du-Lac Cedex, France

E-mail address: `Frederic.Bihan@univ-savoie.fr`